

Moving Beyond Digitization to Compliance

Challenges Hospitals Face on Their Journey

INTRODUCTION

The COVID-19 pandemic accelerated digital transformation within the healthcare industry, from the adoption of telehealth to implementing remote workforce policies in an attempt to keep individuals safe from the virus. As a result, healthcare organizations had to adapt to the unprecedented challenges associated with remote services and keep up with the rise in cyber threats and comply with healthcare regulations. Pondurance commissioned Xtelligent Healthcare Media to survey IT, cybersecurity, and privacy professionals in hospitals to further understand the cybersecurity challenges and needs hospitals face in a digital world.

Together, Pondurance and Xtelligent reviewed the responses of 50 professionals across a variety of hospitals, and our research found that these professionals have a deep insight into the security and privacy challenges at their respective organizations.

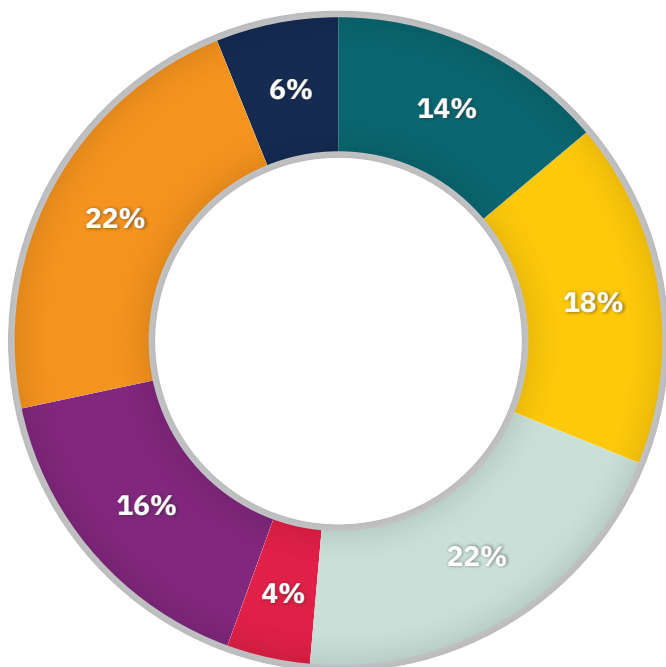
In this whitepaper, we will answer these questions and more:

- What are the leading cybersecurity and privacy challenges before, during, and after COVID-19?
- What changes did hospitals make to adapt to a more digital health environment?
- What challenges should hospitals anticipate in the next six months?

PATIENTS ARE THE DRIVING FORCE BEHIND DIGITAL ACCELERATION

Patients continue to be the driving force behind digital acceleration. They want their healthcare experience to be effortless. The pandemic accelerated telehealth, which made it more accessible, in most cases, for individuals to get nearly the same level of care at home via computer screen instead of going into the doctor's office. As patients demand more digital services, this too can create a greater attack surface for hospitals.

As more digital tools and patient portals are developed to improve patient satisfaction, it can also broaden the attack surface, including potential access to protected health information — either resulting in a data breach or HIPAA penalties. Hospitals need broader views of their digital environment, and its IT department will continue to be a critical asset in digital acceleration.



- Administration
- Cybersecurity
- Data Security
- HIPAA Compliance
- IT Infrastructure
- IT Security
- Privacy

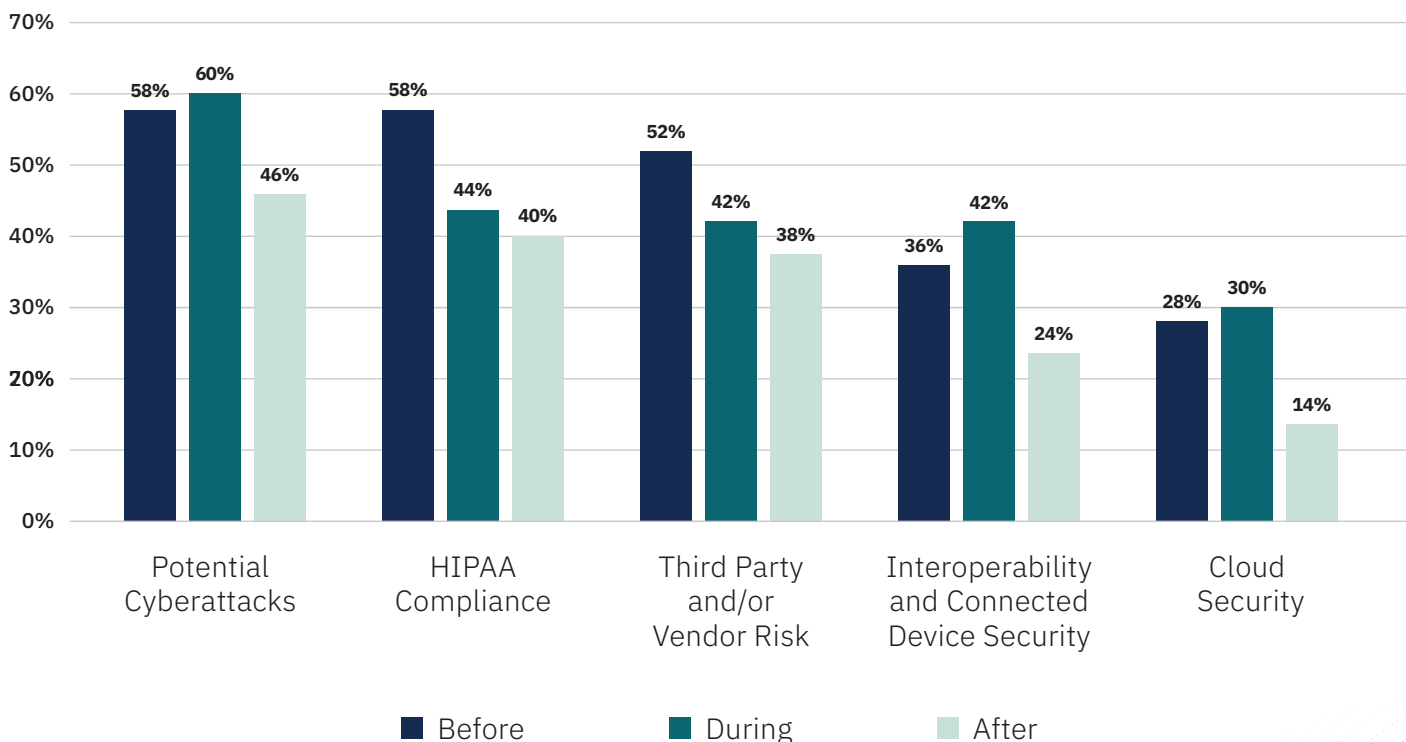
CYBERSECURITY AND PRIVACY CHALLENGES

It is no surprise that hospitals of all sizes have fallen victim to cyberattacks, and it continues to be a top concern for leaders regardless of the COVID-19 pandemic. Hospitals process, store, maintain, and transmit massive amounts of sensitive electronic medical records (EMR) that attract cybercriminals. The data collected consists of personal and financial information, Social Security numbers, and health insurance data, all belonging to one individual, creating an all-in-one package of information for attackers to sell on the dark web.

According to our results, hospitals were most concerned with potential cyberattacks and HIPAA compliance before the pandemic.

During the COVID-19 pandemic, cyberattacks on hospitals significantly increased, impacting valuable resources, patient care, and safety and disrupting business operations. According to our respondents, interoperability and connected device security led to cybersecurity and privacy challenges amid the pandemic. A distributed work environment opens up new avenues to exploit, such as remote desktop connectivity if the IT department needs to service a staff member's laptop or computer. Furthermore, home internet connections are less secure, and attackers have an easier entry point into the hospital's network.

According to 46% of our respondents, post-pandemic, the most significant area of concern remains cyberattacks. Even though hospitals have adapted to telehealth communications as an easier way to interact with patients, there is still a risk to patient information and other HIPAA-covered information, not to mention the hospital's network, if these systems are improperly secured.



CHANGES TO MATURE CYBERSECURITY

To prepare for a more digital health environment, hospitals invest in cybersecurity to stay one step ahead of attackers. More than half, 52% of our respondents are increasing monitoring and increasing the investment in cybersecurity tools. Another 50% are increasing their staff to keep up with these investments.

The results from this study prove that hospitals are focusing on maturing their cybersecurity infrastructure and investing their funding where it matters most — people, processes, and technology. Leveraging technology to achieve 24/7 monitoring, detection, and response and implementing signature-less endpoint detection and response are smart investments that healthcare executives can put toward defending their networks and assuring patient care.

These new investments are common pain points that other organizations struggle with within today's cybersecurity landscape. Often, organizations must choose whether to invest in cybersecurity tools or build an internal security operations center (SOC). The cost to do either can be challenging for small to midsize organizations.

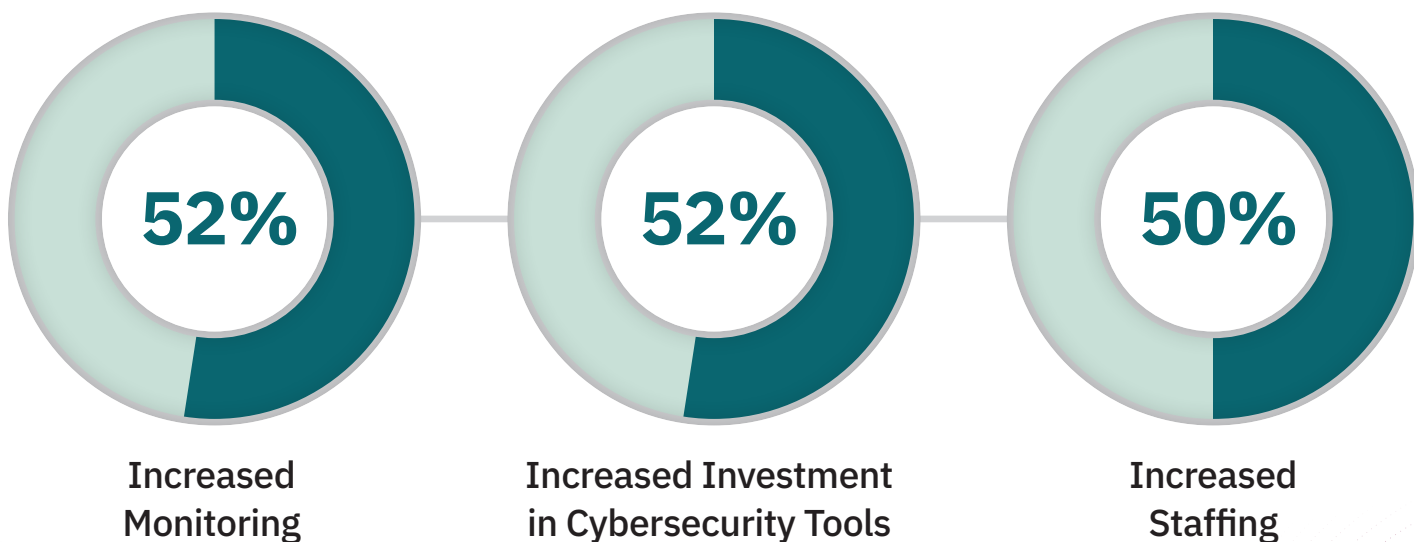
Over half of our respondents, 54%, say the COVID-19 pandemic has increased their cybersecurity budget. But cybersecurity still accounts for less than 10% of a

hospital's overall budget. As budgets steadily increase, hospitals can turn to managed detection and response (MDR) services to gain visibility into the most vulnerable aspects of their network and devices. At the same time, an SOC can act as an extension of its security team to ensure security alerts are quickly triaged.

WHAT'S NEXT FOR DIGITIZATION?

As technology advances in the healthcare industry, digital acceleration is not slowing down anytime soon. According to our survey, selecting the right cybersecurity technology and hiring qualified cybersecurity staff are the biggest challenges hospitals anticipate in the next six months. As hospitals begin to search for a new vendor, they must find one that works best for their healthcare infrastructure. In addition, they should identify whether the vendor specializes in the complex healthcare landscape, integrates with the current technology stack, or monitors their cloud environments.

Hospitals searching for an MDR vendor need to find the right one to fit seamlessly into the healthcare organization and existing security protocols and provide 360-degree visibility. The vendor must have deep experience working with the complex IT landscape, medical devices and endpoints, and healthcare infrastructure so hospitals can stay one step ahead of attackers.



CONCLUSION

Hospitals are working to improve their cybersecurity and compliance strategies to better prepare for a hybrid world. The shift to compliance requires that hospitals protect EMR stored, maintained, and transmitted through applications, networks, and devices.

Our survey reveals that IT, cybersecurity, and privacy professionals in the hospitals we surveyed are aware of the risks that digitization can have on compliance but recognize they cannot solve this problem alone. Investing in the right people and technology regardless of before, during, or after the COVID-19 pandemic can help hospitals keep pace with digitization and customer preferences.



ABOUT PONDURANCE

Pondurance delivers world-class [MDR](#) services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your team can focus on what matters the most.

Pondurance experts include seasoned security operations analysts, [digital forensics and incident response](#) professionals, and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment, and more unified risk.